Plateaued函数的构造方法研究

孙天锋* 胡 斌 杨 阳
(信息工程大学 郑州 450001)

摘 要：Plateaued函数在密码学及编码等领域有着极其重要的应用，该文提出一种Plateaued函数的直接构造方法，研究了由该方法构造的Plateaued函数的密码学性质，证明了现有的直接构造方法可归约到本构造方法。

关键词：布尔函数；Plateaued函数；非线性度；弹性阶
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2018)10-2352-06
DOI: 10.11999/JEIT170965

Research on the Construction of Plateaued Functions

SUN Tianfeng HU Bin YANG Yang
(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: Plateaued functions play a significant role in cryptography, coding theory and so on. In this paper, a new primary construction of plateaued function is given. Some cryptographic properties of the constructed plateaued functions are studied. It is shown that the existing primary constructions of plateaued function can be reduced to the proposed construction.

Key words: Boolean function; Plateaued function; Nonlinearity; Resiliency

1 引言

众所周知，密码函数是序列密码和分组密码中一个重要的密码变换环节，在密码系统的设计中起着举足轻重的作用。为了能够有效抵抗各种密码攻击，密码函数应当具有良好的密码学性质。不同的密码系统侧重的密码学性质不同，但非线性度和弹性阶是两个必须要考虑的性质。Maitra和Sarkar在文献[1]中指出，非线性度和弹性阶相互制约。只有Plateaued函数[2]能达到两者最好的折中。Plateaued函数是包含Bent函数[3]和部分Bent函数[4]的更大的函数类，可具有高非线性度、一定的弹性阶、良好的传播特性，而且可以不具有非零的线性结构，是一类密码学性质优良的函数类。因此，对Plateaued函数构造方法的研究成为一个十分必要的研究课题。

密码函数的构造方法主要分两类：直接构造方法和二次构造方法。关于Plateaued函数直接构造方法的研究成果较少，大多由Bent函数的构造方法推广得来，其中Bent函数两种主要的直接构造方法为文献[5]和文献[6]。之后文献[7]扩展了文献[6]中的构造方法，提出了一种关于Plateaued函数的新的直接构造方法。对于Plateaued函数的其他直接构造方法，可参考文献[8–10]。函数的二次构造方法对于改良函数某些特定的密码学性质具有极其重要的意义，文献[11]推广了间接和(indirect sum)的概念，提出了一种Plateaued函数的二次构造方法；文献[12]通过级联两个Bent函数，给出了一种具有高非线性度且无线性结构的Plateaued函数的构造方法；文献[13]通过固定Bent函数某个变元的值，将一个Bent函数分解为两个Plateaued函数，并利用函数的间接和，给出了一种Plateaued函数二次构造方法。对于Plateaued函数的其他二次构造方法，可参考文献[14–16]。

本文主要对Plateaued函数的直接构造方法进行研究，并分析其相关密码学性质。

2 预备知识

本文用F_2表示二元域，F_2^n表示F_2上的n维向量空间。n元布尔函数为F_2^n到F_2的映射，用B_n表示所有n元布尔函数构成的集合。实数上的加法运算记为$+$和Σ_i，二元域上的加法运算记为$\oplus$和$\oplus_i$。任意$f\in B_n$均可由其代数标准型唯一表示，即

$$f(\boldsymbol{x})=f(x_1,x_2,\cdots,x_n)=\mathop{\oplus}_{\boldsymbol{u}\in F_2^n}\lambda_{\boldsymbol{u}}\left(\prod_{i=1}^{n}x_i^{u_i}\right)$$

收稿日期：2017-10-19；改回日期：2018-06-27；网络出版：2018-07-30
*通信作者： 孙天锋 (enjoy2152013@163.com)
基金项目：国家自然科学基金(61502532)
Foundation Item: The National Natural Science Foundation of China (61502532)

其中，$\lambda_{\boldsymbol{u}} \in F_2$。函数$f(\boldsymbol{x})$的代数次数记为$\deg(f)$，且

$$\deg(f)=\max_{\boldsymbol{u}\in F_2^n}\{wt(\boldsymbol{u}):\lambda_{\boldsymbol{u}}\neq 0\}$$

其中，$wt(\boldsymbol{u})$为向量$\boldsymbol{u}$的汉明重量。当$\deg(f)=1$时，称$f(\boldsymbol{x})$为仿射函数，用A_n表示n元仿射函数构成的集合，特别地，当$\lambda_0=0$时，称$f(x)$为线性函数，用L_n表示n元仿射函数构成的集合。

函数$f\in B_n$在$\boldsymbol{\omega}\in F_2^n$点的Walsh谱为

$$W_f(\boldsymbol{\omega})=\sum_{\boldsymbol{x}\in F_2^n}(-1)^{f(\boldsymbol{x})\oplus\boldsymbol{\omega}\cdot\boldsymbol{x}}$$

其中，$\boldsymbol{\omega}\cdot\boldsymbol{x}$为二者的点积。$f(\boldsymbol{x})$的Walsh谱满足能量守恒定理，即

$$\sum_{\boldsymbol{\omega}\in F_2^n}W_f(\boldsymbol{\omega})^2=2^{2n}$$

$f(\boldsymbol{x})$的非线性度N_f与其Walsh谱之间满足关系：

$$N_f=2^{n-1}-\frac{1}{2}\max_{\boldsymbol{\omega}\in F_2^n}|W_f(\boldsymbol{\omega})|$$

由能量守恒定理可知，$N_f\le 2^{n-1}-2^{n/2-1}$，称非线性度为$2^{n-1}-2^{n/2-1}$的n元布尔函数为Bent函数，显然，n必为偶数。

定义1[2] 设$f\in B_n$，如果存在一个偶数r，使得

$$\#\{\boldsymbol{\omega}\in F_2^n:W_f(\boldsymbol{\omega})\neq 0\}=2^r$$

且对任意的$\boldsymbol{\omega}\in F_2^n$，$W_f(\boldsymbol{\omega})=0$或$\pm 2^{n-r/2}$，则称$f(\boldsymbol{x})$为$r$阶Plateaued函数。

设$f\in B_n$，则$f(\boldsymbol{x})$为m阶弹性函数的充要条件为对任意的$\boldsymbol{\omega}\in F_2^n$，$0\le wt(\boldsymbol{\omega})\le m$，有$W_f(\boldsymbol{\omega})=0$。

定义2[17] 设$f\in B_n$为2次函数，则其双线性函数定义为

$$B_f(\boldsymbol{x},\boldsymbol{y})=f(\boldsymbol{0})\oplus f(\boldsymbol{x})\oplus f(\boldsymbol{y})\oplus f(\boldsymbol{x}\oplus\boldsymbol{y})$$

其根空间$\mathrm{rad}(f)$定义为

$$\mathrm{rad}(f)=\{\boldsymbol{x}\in F_2^n:\forall\boldsymbol{y}\in F_2^n,B_f(\boldsymbol{x},\boldsymbol{y})=0\}$$

下面引理1给出了2次函数Walsh谱与其根空间之间的关系。

引理1[17] 2次函数$f\in B_n$的Walsh谱分布由其根空间$\mathrm{rad}(f)$的维数t唯一确定，如表1所示。

下面介绍几类关于Plateaued函数的函数结构。

定义3[7] 设$n=r+s$，r和s为任意正整数，ϕ为F_2^s到F_2^r的一个映射，g为F_2^s上的布尔函数，则Maiorana-McFarland型函数定义为

$$f_{\mathrm{MM}}(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\cdot\phi(\boldsymbol{y})\oplus g(\boldsymbol{y})\tag{1}$$

其中，$\boldsymbol{x}\in F_2^r,\boldsymbol{y}\in F_2^s$。简记该函数结构为MM型。

下面引理2给出其构成Plateaued函数的充分条件。

引理2[7] 令$f_{\mathrm{MM}}\in B_n$为MM型函数，则

(1)若映射ϕ为单射，则$f_{\mathrm{MM}}(\boldsymbol{x},\boldsymbol{y})$为$2s$阶Plateaued函数；

(2)若映射ϕ为2对1映射，则$f_{\mathrm{MM}}(\boldsymbol{x},\boldsymbol{y})$为$2s-2$阶Plateaued函数。

文献[10]中利用级联函数真值表的方法，给出了一种Plateaued函数的直接构造方法，该方法描述如下：

令t和k为正整数且$k<2^t<2^k$，$E\subseteq F_2^k$，$\#E=2^t$且F_2^k上任意非零线性函数限制在E上不为常数。对任意的$\boldsymbol{e}_i\in E$，令γ_i为线性函数$\boldsymbol{x}\cdot\boldsymbol{e}_i$的真值表，则以$\gamma_0\gamma_1\cdots\gamma_{2^t-1}$为真值表的函数$f\in B_{k+t}$为$2t$阶Plateaued函数。

该构造方法已被证明属于MM型函数结构[9]，即本质为仿射函数的级联，而仿射函数是一类性质较弱的函数，为了弥补该缺点，下面介绍两种级联2次函数的函数结构。

定义4[8] 令n和r为任意正整数，且$r<n$，$t=\lfloor r/2\rfloor$，$s=n-r$。令ψ为F_2^s到F_2^t的一个映射，$\psi_1,\psi_2,\cdots,\psi_t$为其坐标函数，令$\phi$为$F_2^s$到$F_2^r$的一个映射，$\phi_1,\phi_2,\cdots,\phi_r$为其坐标函数，$g$为$F_2^s$上的布尔函数，定义

$$f_{\mathrm{MD}}(\boldsymbol{x},\boldsymbol{y})=\oplus_{i=1}^{t}x_{2i-1}x_{2i}\psi_i(\boldsymbol{y})\oplus\boldsymbol{x}\cdot\phi(\boldsymbol{y})\oplus g(\boldsymbol{y})\tag{2}$$

其中，$\boldsymbol{x}\in F_2^r,\boldsymbol{y}\in F_2^s$。简记该函数结构为MD型。显然，当$\psi$为零映射时，MM型函数与MD型函数相同。

引理3[8] 令$f_{\mathrm{MD}}\in B_n$为MD型函数，对任意的$\boldsymbol{a}\in F_2^r$，定义集合

$$E_{\boldsymbol{a}}=\begin{cases}\{\boldsymbol{y}\in F_2^s:\forall i\le t,\psi_i(\boldsymbol{y})=a_{2i-1}\\ \Rightarrow\phi_{2i-1}(\boldsymbol{y})=a_{2i-1},\phi_{2i}(\boldsymbol{y})=a_{2i}\},\\ \quad r\text{为偶数}\\ \{\boldsymbol{y}\in F_2^s:\forall i\le t,\psi_i(\boldsymbol{y})=a_{2i-1}\\ \Rightarrow\phi_{2i-1}(\boldsymbol{y})=a_{2i-1},\phi_{2i}(\boldsymbol{y})=a_{2i};\phi_r(\boldsymbol{y})s=a_r\},\\ \quad r\text{为奇数}\end{cases}$$

若对任意的$\boldsymbol{y}\in F_2^s$，$\psi(\boldsymbol{y})$的汉明重量为r_0，则

(1)若对任意的$\boldsymbol{a}\in F_2^r$，$\#E_{\boldsymbol{a}}=0$或1，则$f_{\mathrm{MD}}(x,y)$为$2(s+r_0)$阶Plateaued函数；

(2)若对任意的$\boldsymbol{a}\in F_2^r$，$\#E_{\boldsymbol{a}}=0$或2，则$f_{\mathrm{MD}}(x,y)$为$2(s+r_0-1)$阶Plateaued函数。

表 1　谱值与根空间维数的关系

$W_f(\boldsymbol{\omega})$	$\boldsymbol{\omega}$的个数
0	2^n-2^{n-t}
$2^{(n+t)/2}$	$2^{n-t-1}+(-1)^{f(0)}2^{(n-t-2)/2}$
$-2^{(n+t)/2}$	$2^{n-t-1}-(-1)^{f(0)}2^{(n-t-2)/2}$

定义5[9] 设$n=r+s$，r和s为任意正整数，ϕ_1,ϕ_2,ϕ_3是F_2^s到F_2^r的3个映射，g为F_2^s上的布尔函数，定义

$$f_{\mathrm{Q}}(\boldsymbol{x},\boldsymbol{y})=(\boldsymbol{x}\cdot\phi_1(\boldsymbol{y}))(\boldsymbol{x}\cdot\phi_2(\boldsymbol{y}))\oplus\boldsymbol{x}\cdot\phi_3(\boldsymbol{y})\oplus g(\boldsymbol{y}) \tag{3}$$

其中，$\boldsymbol{x}\in F_2^r,\boldsymbol{y}\in F_2^s$。简记该函数结构为Q型。以下引理给出了Q型函数构成Plateaued函数的充分条件。

引理4[9] 令$f_{\mathrm{Q}}(\boldsymbol{x},\boldsymbol{y})\in B_n$为Q型函数，且对任意的$\boldsymbol{y}\in F_2^s$，向量$\phi_1(\boldsymbol{y})$和$\phi_2(\boldsymbol{y})$线性无关。若当$\boldsymbol{y}$遍历$F_2^s$时，$\phi_3(\boldsymbol{y})+<\phi_1(\boldsymbol{y}),\phi_2(\boldsymbol{y})>$中的元素两两不相等，则函数$f_{\mathrm{Q}}(\boldsymbol{x},\boldsymbol{y})$为$2s+2$阶Plateaued函数。

引理5[9] 令$f_{\mathrm{Q}}(\boldsymbol{x},\boldsymbol{y})\in B_n$为Q型函数，且对任意的$\boldsymbol{y}\in F_2^s$，$\phi_2(\boldsymbol{y})\neq 0$。定义以下两个集合：

$$F_a'=\{\boldsymbol{y}\in F_2^s:\phi_1(\boldsymbol{y})与\phi_2(\boldsymbol{y})线性无关;\ \boldsymbol{a}\in\phi_3(\boldsymbol{y})+<\phi_1(\boldsymbol{y}),\phi_2(\boldsymbol{y})>\}$$

$$F_a''=\{\boldsymbol{y}\in F_2^s:\phi_1(\boldsymbol{y})与\phi_2(\boldsymbol{y})线性相关;\ \boldsymbol{a}=\phi_3(\boldsymbol{y})+\phi_1(\boldsymbol{y})\}$$

若对任意的$\boldsymbol{a}\in F_2^r$，$\#F_a'+2\#F_a''=0$或2，则函数$f_{\mathrm{Q}}(\boldsymbol{x},\boldsymbol{y})$是$2s$阶Plateaued函数。

3 新型Plateaued函数结构

MM型函数采用级联仿射函数的方式，MD型和Q型函数采用级联特定形式的2次函数的方式，这3类函数结构的Walsh谱均易于计算。本节给出一种级联一般形式2次函数的函数结构，其谱值也易于计算。

令$\boldsymbol{A}=(a_{ij})_{nn},\boldsymbol{B}=(b_{ij})_{nn},\boldsymbol{C}=(c_{ij})_{nn},\cdots$表示矩阵，$\Omega_t$为所有$t$阶上三角矩阵构成的集合。对任意的2次函数$f\in B_n$且$f(\boldsymbol{0})=0$，其代数标准型为

$$f(\boldsymbol{x})=\bigoplus_{i=1}^{n}\alpha_i x_i\oplus\bigoplus_{1\le i<j\le n}\alpha_{i,j}x_ix_j$$

也可将其表示为

$$f(\boldsymbol{x})=(x_1,x_2,\cdots,x_n)\boldsymbol{A}(x_1,x_2,\cdots,x_n)^{\mathrm{T}} \tag{4}$$

其中，$\boldsymbol{A}\in\Omega_n$，$a_{ii}=\alpha_i$，$a_{ij}=\alpha_{i,j}$。

通过级联式(4)中的2次函数，给出下面的函数结构，记为TF型函数结构。

定义6 设$n=r+s$，r和s为任意正整数，则TF型函数定义为

$$f_{\zeta,g}(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\zeta(\boldsymbol{y})\boldsymbol{x}^{\mathrm{T}}\oplus g(\boldsymbol{y}) \tag{5}$$

其中，$\boldsymbol{x}\in F_2^r,\boldsymbol{y}\in F_2^s$，$\zeta$为$F_2^s$到集合$\Omega_r$的一个映射，$g$为$F_2^s$上的布尔函数。

下面给出TF型函数的谱值计算定理。

定理1 令$f_{\zeta,g}\in B_n$为TF型函数，对任意的$\boldsymbol{x}\in F_2^r,\boldsymbol{y}\in F_2^s$，令$\zeta(\boldsymbol{y})=A_{\boldsymbol{y}}\in\Omega_r$，$h_{\boldsymbol{y}}(\boldsymbol{x})=\boldsymbol{x}\boldsymbol{A}_{\boldsymbol{y}}\boldsymbol{x}^{\mathrm{T}}$，则对任意的$(\boldsymbol{a},\boldsymbol{b})\in F_2^r\times F_2^s$，有

$$W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})=\sum_{\boldsymbol{y}\in F_2^s}\xi_{\boldsymbol{a},\zeta}(\boldsymbol{y})2^{(2r-R(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}}))/2}(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}$$

其中，$R(\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}})$表示矩阵$\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}}$的秩，$\xi_{a,\zeta}$为$F_2^s$到$\{0,1,-1\}$的一个映射：

$$\xi_{\boldsymbol{a},\zeta}(\boldsymbol{y})=\begin{cases}0, & W_{h_{\boldsymbol{y}}}(\boldsymbol{a})=0\\ 1, & W_{h_{\boldsymbol{y}}}(\boldsymbol{a})>0\\ -1, & W_{h_{\boldsymbol{y}}}(\boldsymbol{a})<0\end{cases}$$

证明 由定义2，函数$h_{\boldsymbol{y}}(\boldsymbol{x})$的双线性函数为

$$\begin{aligned}B_{h_{\boldsymbol{y}}}(\boldsymbol{x},\boldsymbol{z})&=h_{\boldsymbol{y}}(\boldsymbol{0})\oplus h_{\boldsymbol{y}}(\boldsymbol{x})\oplus h_{\boldsymbol{y}}(\boldsymbol{z})\oplus h_{\boldsymbol{y}}(\boldsymbol{x}\oplus\boldsymbol{z})\\&=0\oplus\boldsymbol{x}\boldsymbol{A}_{\boldsymbol{y}}\boldsymbol{x}^{\mathrm{T}}\oplus\boldsymbol{z}\boldsymbol{A}_{\boldsymbol{y}}\boldsymbol{z}^{\mathrm{T}}\oplus(\boldsymbol{x}\oplus\boldsymbol{z})\boldsymbol{A}_{\boldsymbol{y}}(\boldsymbol{x}\oplus\boldsymbol{z})^{\mathrm{T}}\\&=\boldsymbol{x}(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}})\boldsymbol{z}^{\mathrm{T}}\end{aligned}$$

其根空间为

$$\begin{aligned}\mathrm{rad}(h_{\boldsymbol{y}})&=\{\boldsymbol{x}\in F_2^r:\forall\boldsymbol{z}\in F_2^r,B_{h_{\boldsymbol{y}}}(\boldsymbol{x},\boldsymbol{z})=0\}\\&=\{\boldsymbol{x}\in F_2^r:\forall\boldsymbol{z}\in F_2^r,\boldsymbol{x}(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}})\boldsymbol{z}^{\mathrm{T}}=0\}\\&=\{\boldsymbol{x}\in F_2^r:\boldsymbol{x}(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}})=\boldsymbol{0}\}\end{aligned}$$

故$\mathrm{rad}(h_{\boldsymbol{y}})$的维数为$r-R(\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}})$。

由引理1及映射$\xi_{\boldsymbol{a},\zeta}$的定义，对任意的$(\boldsymbol{a},\boldsymbol{b})\in F_2^r\times F_2^s$，有

$$\begin{aligned}W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})&=\sum_{\boldsymbol{x}\in F_2^r,\boldsymbol{y}\in F_2^s}(-1)^{f_{\zeta,g}(\boldsymbol{x},\boldsymbol{y})\oplus\boldsymbol{a}\cdot\boldsymbol{x}\oplus\boldsymbol{b}\cdot\boldsymbol{y}}\\&=\sum_{\boldsymbol{y}\in F_2^s}(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}\sum_{x\in F_2^r}(-1)^{\boldsymbol{x}\zeta(\boldsymbol{y})\boldsymbol{x}^{\mathrm{T}}\oplus\boldsymbol{a}\cdot\boldsymbol{x}}\\&=\sum_{\boldsymbol{y}\in F_2^s}\xi_{\boldsymbol{a},\zeta}(\boldsymbol{y})2^{(r+(r-R(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}})))/2}(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}\\&=\sum_{\boldsymbol{y}\in F_2^s}\xi_{\boldsymbol{a},\zeta}(\boldsymbol{y})2^{(2r-R(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}}))/2}(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}\end{aligned}$$

证毕

由此给出Plateaued函数的构造定理。

定理2 令$f_{\zeta,g}\in B_n$为TF型函数，假定对任意的$\boldsymbol{y}\in F_2^s$，$R(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}})$保持不变，记为$t_0$。定义集合

$$F_{\boldsymbol{a}}=\{\boldsymbol{y}\in F_2^s:\xi_{\boldsymbol{a},\zeta}(\boldsymbol{y})\neq 0\},\ \boldsymbol{a}\in F_2^r$$

则

(1) 若对任意的$\boldsymbol{a}\in F_2^r$，$\#F_{\boldsymbol{a}}=0$或1，则函数$f_{\zeta,g}(\boldsymbol{x},\boldsymbol{y})$是$2s+t_0$阶Plateaued函数；

(2) 若对任意的$\boldsymbol{a}\in F_2^r$，$\#F_{\boldsymbol{a}}=0$或2，则函数$f_{\zeta,g}(\boldsymbol{x},\boldsymbol{y})$是$2s+t_0-2$阶Plateaued函数。

证明 由于对任意的$\boldsymbol{y}\in F_2^s$，$R(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}})$保持

不变，则由定理1可知，对任意的$(\boldsymbol{a},\boldsymbol{b})\in F_2^r\times F_2^s$，有

$$W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})=\sum_{\boldsymbol{y}\in F_2^s}\xi_{\boldsymbol{a},\zeta}(\boldsymbol{y})2^{(2r-R(\boldsymbol{A}_{\boldsymbol{y}}\oplus\boldsymbol{A}_{\boldsymbol{y}}^{\mathrm{T}}))/2}(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}$$
$$=2^{r-t_0/2}\sum_{\boldsymbol{y}\in F_2^s}\xi_{\boldsymbol{a},\zeta}(\boldsymbol{y})(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}$$

若对任意的$\boldsymbol{a}\in F_2^r$，$\#F_{\boldsymbol{a}}=0$或1，则$W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})$为0或$\pm(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}2^{r-t_0/2}=\pm2^{r-t_0/2}$，即$f_{\zeta,g}(\boldsymbol{x},\boldsymbol{y})$是$2s+t_0$阶Plateaued函数。

同理可证条件(2)。　　证毕

注1 由定理1及定理2可知，当对任意的$\boldsymbol{a}\in F_2^r$，$\#F_{\boldsymbol{a}}=0$或1成立时，有

$$\sum_{\boldsymbol{a}\in F_2^r,\boldsymbol{y}\in F_2^s}W_{h_y}^2(\boldsymbol{a})\le 2^{3r-t_0}$$
$$\sum_{\boldsymbol{a}\in F_2^r,\boldsymbol{b}\in F_2^s}W_f^2(\boldsymbol{a},\boldsymbol{b})\le 2^{3r+s-t_0}$$

由能量守恒定理可知，

$$2^{s+2r}\le 2^{3r-t_0},\ 2^{2s+2r}\le 2^{3r+s-t_0}$$

由此可知，$s\le r-t_0$。同理可得，当对任意的$\boldsymbol{a}\in F_2^r$，$\#F_{\boldsymbol{a}}=0$或2成立时，有$s\le r-t_0+2$。

以下记满足条件(1)的函数为TF_1型Plateaued函数，满足条件(2)的函数为TF_2型Plateaued函数。

由非线性度和谱值之间的关系可知，TF_1型Plateaued函数的非线性度为$2^{n-1}-2^{(2r-t_0)/2-1}$；TF_2型Plateaued函数的非线性度为$2^{n-1}-2^{(2r-t_0)/2}$。

由于TF型Plateaued函数本质为级联一般形式的2次函数，故其代数次数$\le s+2$。

下面两个定理分别研究了TF_1型和TF_2型Plateaued函数的弹性阶。

定理3 令$f_{\zeta,g}\in B_n$为TF_1型Plateaued函数，集合

$$D=\{\boldsymbol{a}\in F_2^r:\text{存在}\boldsymbol{y}\in F_2^s\text{使得}\xi_{a,\zeta}(\boldsymbol{y})\ne 0\}$$

整数k为集合D中元素汉明重量的最小值，则函数$f_{\zeta,g}$的弹性阶为$k-1$且

$$k\le\max\left\{t\in N:\sum_{i=0}^{t}\begin{pmatrix}r\\i\end{pmatrix}\le 2^r-\#D\right\}+1$$

证明 由$f_{\zeta,g}\in B_n$为TF_1型Plateaued函数，故对任意的$\boldsymbol{a}\in F_2^r$，$\#F_{\boldsymbol{a}}=0$或1。由集合D的定义可知，函数$f_{\zeta,g}$的弹性阶$\le k-1$。由定理1和定理2，对任意的$(\boldsymbol{a},\boldsymbol{b})\in F_2^r\times F_2^s$，$W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})=\pm2^{r-t_0/2}$当且仅当$\boldsymbol{a}\in D$。若$wt(\boldsymbol{a},\boldsymbol{b})\le k-1$，则$wt(\boldsymbol{a})\le k-1$，从而$\boldsymbol{a}\notin D$，故$W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})=0$，从而函数$f_{\zeta,g}$的弹性阶$\ge k-1$。

因此，函数$f_{\zeta,g}$的弹性阶为$k-1$。

由集合D和整数k的定义，汉明重量$\le k-1$的向量在集合D^c中，故有

$$\sum_{i=0}^{k-1}\begin{pmatrix}r\\i\end{pmatrix}\le 2^r-\#D$$

由此得到

$$k\le\max\{t\in N:\sum_{i=0}^{t}\begin{pmatrix}r\\i\end{pmatrix}\le 2^r-\#D\}+1$$

证毕

定理4 令$f_{\zeta,g}\in B_n$为TF_2型Plateaued函数，集合D和整数k如定理3中定义，则函数$f_{\zeta,g}$的弹性阶为k或$k-1$且

$$k\le\max\left\{t\in N:\sum_{i=0}^{t}\begin{pmatrix}r\\i\end{pmatrix}\le 2^r-\#D\right\}+1$$

证明 由定理1和定理2可知，对任意的$(\boldsymbol{a},\boldsymbol{b})\in F_2^r\times F_2^s$，$W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})=\pm2^{r+1-t_0/2}$当且仅当$\boldsymbol{a}\in D$。若$wt(\boldsymbol{a},\boldsymbol{b})\le k-1$，则$wt(\boldsymbol{a})\le k-1$，从而$\boldsymbol{a}\notin D$，故$W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})=0$。由此可知，函数$f_{\zeta,g}$的弹性阶$\ge k-1$。

取$\boldsymbol{a}\in D$且$wt(\boldsymbol{a})=k$，令$\boldsymbol{y}_1,\boldsymbol{y}_2\in F_2^s$且$\xi_{a,\zeta}(\boldsymbol{y}_1)\ne 0$，$\boldsymbol{\xi}_{a,\zeta}(\boldsymbol{y}_2)\ne 0$。由定理1，对任意的$\boldsymbol{b}\in F_2^s$，限制在$\{\boldsymbol{a}\}\times F_2^s$上的谱值为以下二者之一：

$$\frac{1}{2^{r-t_0/2}}W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})=\pm[(-1)^{g(\boldsymbol{y}_1)\oplus\boldsymbol{b}\cdot\boldsymbol{y}_1}-(-1)^{g(\boldsymbol{y}_2)\oplus\boldsymbol{b}\cdot\boldsymbol{y}_2}]$$
$$=\pm2[\boldsymbol{b}\cdot(\boldsymbol{y}_1\oplus\boldsymbol{y}_2)\oplus g(\boldsymbol{y}_1)\oplus g(\boldsymbol{y}_2)]$$
$$\frac{1}{2^{r-t_0/2}}W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})=\pm[(-1)^{g(\boldsymbol{y}_1)\oplus\boldsymbol{b}\cdot\boldsymbol{y}_1}+(-1)^{g(\boldsymbol{y}_2)\oplus\boldsymbol{b}\cdot\boldsymbol{y}_2}]$$
$$=\pm2\left[\boldsymbol{b}\cdot(\boldsymbol{y}_1\oplus\boldsymbol{y}_2)\oplus g(\boldsymbol{y}_1)\oplus g(\boldsymbol{y}_2)\oplus 1\right]$$

当向量$\boldsymbol{y}_1\ne\boldsymbol{y}_2$时，线性函数$\boldsymbol{b}\cdot(\boldsymbol{y}_1\oplus\boldsymbol{y}_2)$在集合$\{\boldsymbol{b}\in F_2^s:wt(\boldsymbol{b})\le 1\}$上的取值不为常值，从而总存在$\boldsymbol{b}\in F_2^s$，$wt(\boldsymbol{b})\le 1$，使得$W_{f_{\zeta,g}}(\boldsymbol{a},\boldsymbol{b})\ne 0$，从而函数$f_{\zeta,g}$的弹性阶$< k+1$。

因此，函数$f_{\zeta,g}$的弹性阶为k或$k-1$。整数k界的证明与定理3相同，这里不再赘述。　　证毕

4　各类函数结构之间的包含关系

第2节已经说明文献[10]中的函数类可归约到MM型函数，而MM型函数又可归约到MD型函数。本节证明MD型Plateaued函数和Q型Plateaued函数都可归约到TF型Plateaued函数。

首先，给出MD型Plateaued函数的归约证明。定义集合

$$\Omega_r^{\mathrm{MD}}=\{\boldsymbol{A}\in\Omega_r:a_{(2i-1)(2i)},a_{jj}\in F_2,$$
$$1\le i\le t,1\le j\le r;\text{其余}a_{ij}=0\}$$

其中，$t=\lfloor r/2\rfloor$，令ζ_{MD}为F_2^s到Ω_r^{MD}的映射，则函数$f_{\zeta_{\mathrm{MD}},g}(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\zeta_{\mathrm{MD}}(\boldsymbol{y})\boldsymbol{x}^{\mathrm{T}}\oplus g(\boldsymbol{y})$即为MD型函数。

定理5 令函数$f_{\mathrm{MD}}\in B_n$为MD型函数。若对任意的$\boldsymbol{y}\in F_2^s$，$\psi(\boldsymbol{y})$的汉明重量为常数r_0，则对任意的$\boldsymbol{A}\in\Omega_r^{\mathrm{MD}}$，$R(\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}})=2r_0$。

证明 由于仿射函数的双线性函数恒为零函数，这里只考虑映射ψ。

若对任意的$\boldsymbol{y}\in F_2^s$，$\psi(\boldsymbol{y})$的汉明重量为r_0，则向量$(\psi_1(\boldsymbol{y}),\psi_2(\boldsymbol{y}),\cdots,\psi_t(\boldsymbol{y}))$中1的个数为$r_0$，即集合$\{a_{12},a_{34},\cdots,a_{(2t-1)(2t)}\}$中1的个数为$r_0$。

当r_0为偶数时，矩阵$\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}}$为

$$\begin{bmatrix}\begin{matrix}0&a_{12}\\a_{21}&0\end{matrix}&&&\\&\begin{matrix}0&a_{34}\\a_{43}&0\end{matrix}&&\\&&\ddots&\\&&&\begin{matrix}0&a_{(r-1)(r)}\\a_{(r)(r-1)}&0\end{matrix}\end{bmatrix}$$

其中，$a_{12}=a_{21},\cdots,a_{(r-1)(r)}=a_{(r)(r-1)}$。显然，此时有$R(\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}})=2r_0$。同理可证$r_0$为奇数时的情况。 证毕

定理6 MD型Plateaued函数可归约到TF型Plateaued函数。

证明 对任意的$(\boldsymbol{a},\boldsymbol{b})\in F_2^r\times F_2^s$，函数$f_{\mathrm{MD}}$在该点的Walsh谱为

$$W_{f_{\mathrm{MD}}}(\boldsymbol{a},\boldsymbol{b})=\sum_{\boldsymbol{y}\in F_2^s}\sum_{\boldsymbol{x}\in F_2^r}(-1)^{\oplus_{i=1}^t\boldsymbol{x}_{2i-1}\boldsymbol{x}_{2i}\psi_i(\boldsymbol{y})\oplus\boldsymbol{x}\cdot\phi(\boldsymbol{y})\oplus\boldsymbol{a}\cdot\boldsymbol{x}}(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}$$

若对任意的$\boldsymbol{a}\in F_2^r$，有$\#E_{\boldsymbol{a}}=0$或1，则由定理5可知，至多存在一个$\boldsymbol{y}\in F_2^s$使得

$$\left|\sum_{\boldsymbol{x}\in F_2^r}(-1)^{\oplus_{i=1}^t x_{2i-1}\boldsymbol{x}_{2i}\psi_i(\boldsymbol{y})\oplus\boldsymbol{x}\cdot\phi(\boldsymbol{y})\oplus\boldsymbol{a}\cdot\boldsymbol{x}}\right|=2^{r-r_0}$$

由映射ζ_{MD}和集合$F_{\boldsymbol{a}}$的定义可知，$\#F_{\boldsymbol{a}}=0$或1。

同理可证若对任意的$\boldsymbol{a}\in F_2^r$，$\#E_{\boldsymbol{a}}=0$或2，则$\#F_{\boldsymbol{a}}=0$或2。 证毕

下面给出Q型Plateaued函数的归约证明。由于式(3)中的函数$(\boldsymbol{x}\cdot\phi_1(\boldsymbol{y}))(\boldsymbol{x}\cdot\phi_2(\boldsymbol{y}))\oplus\boldsymbol{x}\cdot\phi_3(\boldsymbol{y})$的秩为0或2[9]，定义集合

$$\Omega_r^{\mathrm{Q}}=\{\boldsymbol{A}\in\Omega_r:R(\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}})=0\text{或}2\}$$

令ζ_{Q}为F_2^s到Ω_r^{Q}的一个映射，则函数$f_{\zeta_{\mathrm{Q}},g}(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\zeta_{\mathrm{Q}}(\boldsymbol{y})\boldsymbol{x}^{\mathrm{T}}\oplus g(\boldsymbol{y})$即为Q型函数。

定理7 Q型Plateaued函数可归约到TF型Plateaued函数。

证明 令集合

$$E=\{\boldsymbol{y}\in F_2^s:\phi_1(\boldsymbol{y})\text{和}\phi_2(\boldsymbol{y})\}\text{线性无关}$$

若$E=F_2^s$，则对任意的$\boldsymbol{A}\in\Omega_r^{\mathrm{Q}}$，$R(\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}})=2$；若$E$为空集，则对任意的$\boldsymbol{A}\in\Omega_r^{\mathrm{Q}}$，有$R(\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}})=0$。

对任意的$(\boldsymbol{a},\boldsymbol{b})\in F_2^r\times F_2^s$，函数$f_{\mathrm{Q}}$在该点的Walsh谱为

$$W_{f_{\mathrm{Q}}}(\boldsymbol{a},\boldsymbol{b})=\sum_{\boldsymbol{y}\in F_2^s}\sum_{\boldsymbol{x}\in F_2^r}(-1)^{(\boldsymbol{x}\cdot\phi_1(\boldsymbol{y}))(\boldsymbol{x}\cdot\phi_2(\boldsymbol{y}))\oplus\boldsymbol{x}\cdot\phi_3(\boldsymbol{y})\oplus\boldsymbol{a}\cdot\boldsymbol{x}}(-1)^{g(\boldsymbol{y})\oplus\boldsymbol{b}\cdot\boldsymbol{y}}$$

若对任意的$\boldsymbol{y}\in F_2^s$，$\phi_3(\boldsymbol{y})+<\phi_1(\boldsymbol{y}),\phi_2(\boldsymbol{y})>$中元素两两不相等，则对任意的$\boldsymbol{a}\in F_2^r$，至多存在一个$\boldsymbol{y}\in F_2^s$使得

$$\left|\sum_{\boldsymbol{x}\in F_2^r}(-1)^{(\boldsymbol{x}\cdot\phi_1(\boldsymbol{y}))(\boldsymbol{x}\cdot\phi_2(\boldsymbol{y}))\oplus\boldsymbol{x}\cdot\phi_3(\boldsymbol{y})\oplus\boldsymbol{a}\cdot\boldsymbol{x}}\right|=2^{r-1}$$

由映射ζ_{Q}和集合$F_{\boldsymbol{a}}$的定义可知，$\#F_{\boldsymbol{a}}=0$或1。

令集合$F'_{\boldsymbol{a}}$和$F''_{\boldsymbol{a}}$如引理5中定义，若$\#F'_{\boldsymbol{a}}+2\#F''_{\boldsymbol{a}}=0$或2，则

$$\begin{cases}\#F'_{\boldsymbol{a}}=0\text{或}2\\\#F''_{\boldsymbol{a}}=0\end{cases}\quad\text{或}\quad\begin{cases}\#F'_{\boldsymbol{a}}=0\\\#F''_{\boldsymbol{a}}=0\text{或}1\end{cases}$$

当$\#F'_{\boldsymbol{a}}=0$或2，$\#F''_{\boldsymbol{a}}=0$时，对任意的$\boldsymbol{A}\in\Omega_r^{\mathrm{Q}}$，$R(\boldsymbol{A}\oplus\boldsymbol{A}^{\mathrm{T}})=2$，且对任意的$\boldsymbol{a}\in F_2^r$，存在0或2个$\boldsymbol{y}\in F_2^s$使得

$$\left|\sum_{\boldsymbol{x}\in F_2^r}(-1)^{(\boldsymbol{x}\cdot\phi_1(\boldsymbol{y}))(\boldsymbol{x}\cdot\phi_2(\boldsymbol{y}))\oplus\boldsymbol{x}\cdot\phi_3(\boldsymbol{y})\oplus\boldsymbol{a}\cdot\boldsymbol{x}}\right|=2^{r-1}$$

由映射ζ_{Q}和集合$F_{\boldsymbol{a}}$的定义可知，$\#F_{\boldsymbol{a}}=0$或2。同理可证当$\#F_{\boldsymbol{a}}'=0$，$\#F''_{\boldsymbol{a}}=0$或1时，$\#F_{\boldsymbol{a}}=0$或1。 证毕

注2 TF型函数的函数量为$N(\mathrm{TF})=(2^{(r^2+r)/2})^{2^s}\times2^{2^s}=2^{[(r^2+r)/2+1]2^s}$；MD型函数的函数量为$N(\mathrm{MD})=(2^{2^s})^t\times(2^r)^{2^s}\times2^{2^s}=2^{(t+r+1)2^s}$；Q型函数的函数量为$N(\mathrm{Q})=[(2^r)^{2^s}]^3\times2^{2^s}=2^{(3r+1)2^s}$。可见，$N(\mathrm{TF})\geq N(\mathrm{GMM})$且当$r\geq6$时，$N(\mathrm{TF})>N(\mathrm{Q})$。

下面给出一类不为MD型或Q型的TF型Plateaued函数。

例1 令$n=13$，$s=4$，$r=9$，矩阵$\boldsymbol{A}_1\in\Omega_4$，$\boldsymbol{A}_2\in\Omega_5$为

$$\boldsymbol{A}_1=\begin{bmatrix}0&0&1&0\\0&0&1&1\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

$$\boldsymbol{A}_2=\begin{bmatrix}a_{55}&0&0&0&0\\0&a_{66}&0&0&0\\0&0&a_{77}&0&0\\0&0&0&a_{88}&0\\0&0&0&0&a_{99}\end{bmatrix}$$

其中，$a_{55}, a_{66}, a_{77}, a_{88}, a_{99} \in F_2$，矩阵$\boldsymbol{A} \in \Omega_9$为

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{A}_1 & \boldsymbol{A}_3 \\ \boldsymbol{A}_4 & \boldsymbol{A}_2 \end{bmatrix}$$

其中，$\boldsymbol{A}_3$和$\boldsymbol{A}_4$为全0矩阵，记由满足上述条件的矩阵$\boldsymbol{A}$构成的集合为Ω_9^0。

此时，对任意的$\boldsymbol{A} \in \Omega_9^0$, $R(\boldsymbol{A} \oplus \boldsymbol{A}^{\mathrm{T}}) = 4$。由于$\#\Omega_9^0 = 32 > 16$，可定义$F_2^4$到$\Omega_9^0$的单射，可以验证该单射满足定理2中的条件(1)，即函数$f_{\zeta,g}$为13元12阶Plateaued函数。

显然，对任意的$\boldsymbol{A} \in \Omega_9^0$，有$\boldsymbol{A} \notin \Omega_9^{\mathrm{MD}}$且$\boldsymbol{A} \notin \Omega_9^{\mathrm{Q}}$。

5　结束语

本文提出了一类新型函数结构，即TF型函数，给出了TF型函数构成Plateaued函数的充分条件，分析了该类Plateaued函数的代数次数、非线性度和弹性阶，指出了TF型Plateaued函数是包含MM型、MD型和Q型Plateaued函数的更为一般的函数类。与现有直接构造方法相比，TF型Plateaued函数形式更为一般，需要满足的条件也更为宽泛，此外，TF型函数的函数量更大，能够构造大量与现有函数类不同的Plateaued函数。

参 考 文 献

[1] SARKAR P and MAITRA S. Nonlinearity bounds and constructions of resilient Boolean functions[C]. International Cryptology Conference, California, USA, 2000: 515–532. doi: 10.1007/3-540-44598-6_32.

[2] ZHENG Y L and ZHANG X M. On plateaued functions[J]. *IEEE Transactions on Information Theory*, 2001, 47(3): 1215–1223. doi: 10.1109/18.915690.

[3] Rothaus O S. On bent functions[J]. *Journal of Combinatorial Theory*, 1976, 20(3): 300–305. doi: 10.1016/0097-3165(76)90024-8.

[4] CARLET C. Partially bent functions[J]. *Designs, Codes and Cryptography*, 1993, 3(2): 135–145. doi: 10.1007/BF01388412.

[5] DILLON J F. Elementary Hadamard difference sets[D]. [Ph.D. dissertation], University of Maryland, 1974. doi: 10.13016/M2MS3K194.

[6] MCFARLAND R L. A family of difference sets in noncyclic groups[J]. *Journal of Combinatorial Theory*, 1973, 15(1): 1–10. doi: 10.1016/0097-3165(73)90031-9.

[7] CAMION P, CARLET C, CHARPIN P, *et al*. On Correlation immune functions[C]. International Cryptology Conference, California, USA, 1991: 68–100. doi: 10.1007/3-540-46766-1_6.

[8] CARLET C. A larger Class of Cryptographic Boolean functions via a study of the Marorana-McFarland Construction[C]. International Cryptology Conference, California, USA, 2002: 68–100. doi: 10.1007/3-540-45708-9_35.

[9] CARLET C and PROUFF E. On plateaued functions and their construction[C]. Fast Software Encryption, Lund, Sweden, 2003: 54–73. doi: 10.1007/978-3-540-39887-5_6.

[10] ZHENG Y L and ZHANG X M. Plateaued functions[C]. International Conference on Information and Communications Security, Berlin, Heidelberg, 1999: 284–300. doi: 10.1007/978-3-540-47942-0_24.

[11] ZHANG F R, CARLET C, HU Y P, *et al*. Secondary constructions of highly nonlinear Boolean functions and disjoint spectra plateaued functions[J]. *Information Sciences*, 2014, 283: 94–106. doi: 10.1016/j.ins.2014.06.024.

[12] CUSICK T W. Highly nonlinear plateaued functions[J]. *IET Information Security*, 2017, 11(2): 78–81. doi: 10.1049/iet-ifs.2016.0131.

[13] ZHANG F R, CARLET C, HU Y P, *et al*. New secondary constructions of bent functions[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2016, 27(5): 413–434. doi: 10.1007/s00200-016-0287-6.

[14] HYUN J Y, LEE J, and LEE Y. Explicit criteria for construction of plateaued functions[J]. *IEEE Transactions on Information Theory*, 2016, 62(12): 7555–7565. doi: 10.1109/TIT.2016.2582217.

[15] MESNAGER S, TANG C M, and QI Y F. Generalized plateaued functions and admissible (plateaued) functions[J]. *IEEE Transactions on Information Theory*, 2017, 63(10): 6139–6148. doi: 10.1109/TIT.2017.2715804.

[16] OLMEZ O. Plateaued functions and one-half difference sets[J]. *Designs, Codes and Cryptography*, 2015, 76(3): 537–549. doi: 10.1007/s10623-014-9975-z.

[17] CANTEAUT A, CHARPIN P, and KYUREGHYAN G M. A new class of monomial bent functions[J]. *Finite Fields and Their Applications*, 2008, 14(1): 221–241. doi: 10.1016/j.ffa.2007.02.004.

孙天锋：男，1990年生，博士生，研究方向为密码函数与序列密码理论.

胡　斌：男，1971年生，教授，主要从事密码学与信息安全研究.

杨　阳：女，1980年生，副教授，主要从事密码学与信息安全研究.